EOBR Peer to Peer Communications for Roadside Inspections

Fred Gnuechtel

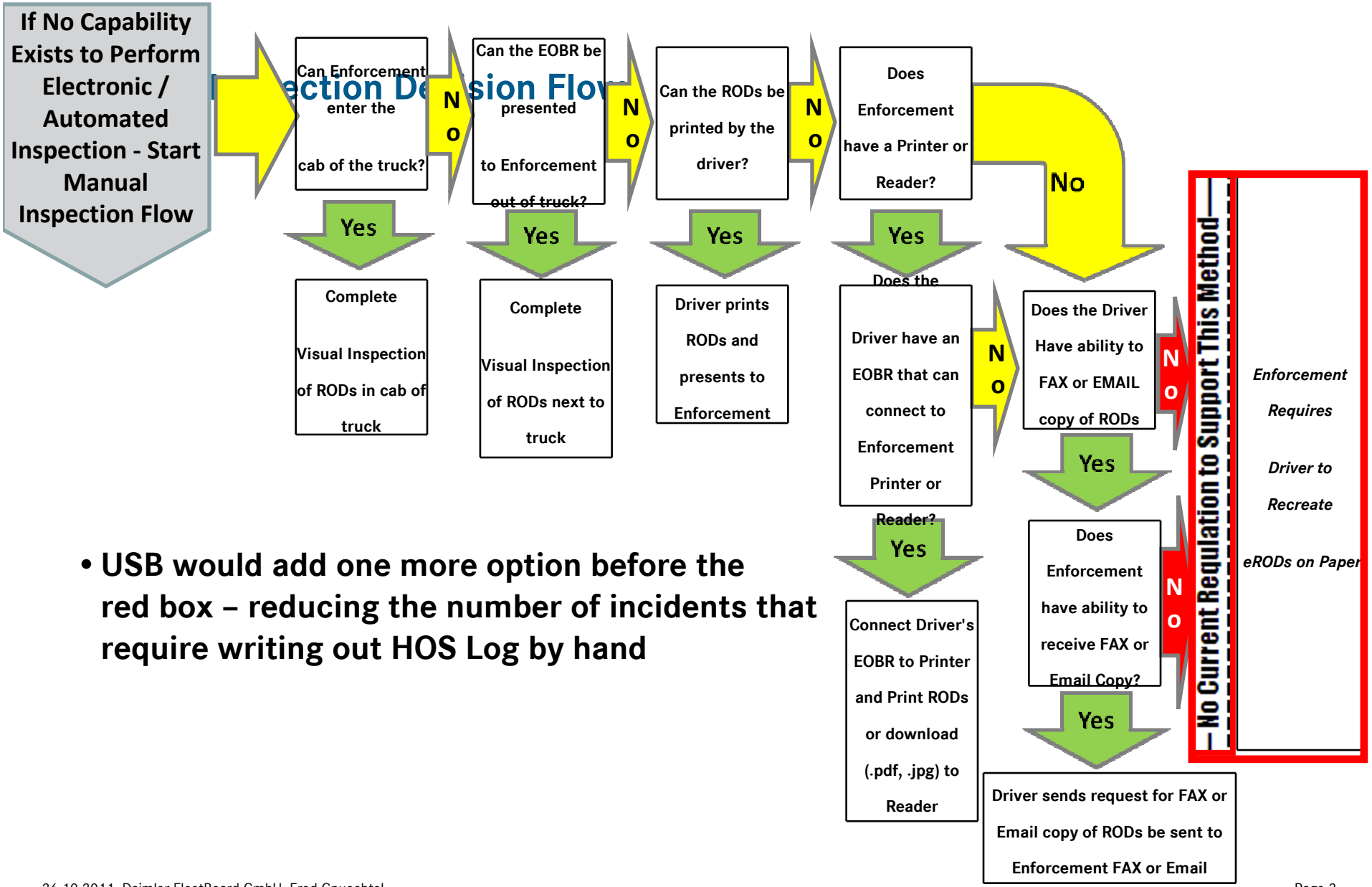
fred.gnuechtel@daimler.com

+1 (512) 947 6228

EOBR Peer to Peer for Roadside Inspections

- USB is a widely available, accepted and easily understood technology
- More straightforward to implement than WiFi or Bluetooth
- Risks can be understood and identified.
    - Malware threats from “infected” USB Memory device
    - Authentication that USB contains real EOBR HOS data
    - Liability created by exchange of the USB Memory device
- “Worst case scenarios” can be anticipated, addressed, contained or eliminated
    - Mitigate the risk to something manageable

• Slide courtesy JB Hunt - Workgroup Report – Manual Inspection



- **USB would add one more option before the red box – reducing the number of incidents that require writing out HOS Log by hand**

Making Peer to Peer via USB a viable solution

- Rather than identify why it should not be used. . .
    - Define a solution that will make it work
    - Define and Address the risks
    - Take it a step at a time.
- Address the “worst case” scenario of zero connectivity

USB Solution Approach

- Most if not all EOBR designs will include USB ports
    - Legitimate software updates
- There will be malicious attacks through USB
    - “Where there is a will there is a way”
    - EOBR designs will have to be designed to anticipate this anyway
    - Not all attacks may be intentional
- Minimize or eliminate effectiveness of malicious attacks
    - Reduce the scope of the risk
    - Reduce the negative impact to a very small percentage of the roadside inspections

Possible USB Solution Definition . . .

- EOBR Manufacturer responsible for ensuring and certifying that the EOBR device will be resistant to attacks and infection from the USB port:
    - Will need to build security into the EOBR design anyway – even if USB Memory not used in peer to peer mode during roadside inspections
    - Only write HOS Logs to USB Memory
    - Do not read anything from unauthenticated USB Memory

USB Solution Definition . . .

- Enforcement uses a separate non network connected device to read the Data file.
    - Stand alone device
    - All certified Enforcement personnel must have the device
        - Additional cost limited to the number of certified personnel
            - Not every truck
            - 10's of thousands – not millions
    - Enforcement Device does not write to the USB Memory
        - Deletes files once reviewed
    - Device does not connect to Enforcement IT network
    - Device does not have an internal battery or read/write memory
    - Device only reads and deletes HOS log files.
    - In case of citation, Enforcement retains the USB Memory device as evidence

USB HOS Log format

- When a vehicle is stopped for an inspection, the Enforcement officer will provide the vehicle driver with:
    - A USB Memory device
    - An Inspection ID or unique identifier.
- The Driver will enter this into the EOBR, and insert a USB Memory device.
- The Driver will request the EOBR generate a copy of the HOS Log.
    - Data can be in either Grid Graph or Flat File – or both
- Format it in the form of a 600 x 400 bitmap (BMP) file.
    - BMP's have no ability to hide malware/executable code
    - Create multiple BMP files if volume of data dictates it.

Enforcement USB Display device

- Enforcement would be equipped with a USB Display device:
  - Based on a commercially available Digital Picture Frame device
    - Device based on consumer grade product
      - Cheap and replaceable instead of ruggedized and expensive
      - Target price < $100.
    - Device optimized to display 600 x 400 color images
    - Reads and displays BMP files only
    - Does not write to USB Memory device
    - Does not store images internally in the USB Display device.
  - Can be transferred to Laptop or back office if allowed

Enforcement inspection of HOS log

- Enforcement receives USB Memory device from vehicle driver
- Plugs in and powers up the Display device (dedicated function = fast boot)
- Inserts the USB Memory device in the USB Display device
- Verifies the Inspection ID and HOS compliance
- If there is an HOS infraction:
    - Retains the BMP files or USB Memory device as evidence
    - Takes appropriate Enforcement action

Conclusion

- Peer to Peer HOS log review is a must for EOBR to be successful
- USB Memory device with a USB Display device for Enforcement meets the need:
    - Provides a cost effective solution for Enforcement
        - $100 per device x 20,000 Enforcement officers = $2.0 M
    - May be implemented to reduce impact of unsecure & unsafe data transfer/review
    - Removes need for paper HOS Log
    - Minimizes impact to currently available EOBR hardware
    - Maintains intent of reducing costs associated with paper data retention
    - Easily adapted to security protocols and encryption that may be adopted later